



DEPARTMENT OF HOMELAND SECURITY

[Docket No. ICEB-2020-0002]

Privacy Act of 1974; System of Records

AGENCY: U.S. Immigration and Customs Enforcement, U.S. Department of Homeland Security.

ACTION: Notice of a Modified System of Records.

SUMMARY: In accordance with the Privacy Act of 1974, the U.S. Department of Homeland Security (DHS) proposes to modify and reissue a current system of records titled, “DHS/U.S. Immigration and Customs Enforcement (ICE)-009 External Investigations System of Records.” This system of records allows the DHS/ICE to collect and maintain records by ICE Homeland Security Investigations (HSI). This system of records covers information related to external audits, inquiries, and investigations pertaining to suspected violations of laws regulating the movement of people and goods into and out of the United States. DHS/ICE is updating this system of records to revise the purpose, update and expand the category of individuals, add new categories of records, modify and add to routine uses, update the records retention policies, and make non-substantive formatting changes.

DATES: Submit comments on or before **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**. This modified system will be effective upon publication. New or modified routine uses will become effective **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**.

ADDRESSES: You may submit comments, identified by docket number ICEB-2020-0002 by one of the following methods:

- Federal e-Rulemaking Portal: <http://www.regulations.gov>. Follow the instructions for submitting comments.
- Fax: 202-343-4010.
- Mail: Constantina Kozanas, Chief Privacy Officer, Privacy Office, U.S. Department of Homeland Security, Washington, D.C. 20528-0655.

Instructions: All submissions received must include the agency name and docket number ICEB-2020-0002. All comments received will be posted without change to <http://www.regulations.gov>, including any personal information provided.

Docket: For access to the docket to read background documents or comments received go to <http://www.regulations.gov>.

FOR FURTHER INFORMATION CONTACT: For general questions please contact:

Jordan Holz, (202) 732-3300, Privacy Officer, U.S. Immigration and Customs Enforcement (ICE), 500 12th Street, SW, Mail Stop 5004, Washington, D.C. 20536. For privacy questions, please contact: Constantina Kozanas, (202) 343-1717, Privacy@hq.dhs.gov, Chief Privacy Officer, Privacy Office, U.S. Department of Homeland Security, Washington, D.C. 20528-0655.

SUPPLEMENTARY INFORMATION:

I. Background

In accordance with the Privacy Act of 1974, 5 U.S.C. sec. 552a, DHS/ICE proposes to modify and reissue a current DHS system of records notice (SORN) titled, “DHS/ICE-009 External Investigations System of Records.” DHS/ICE is updating this system of records to better reflect and clarify the nature of law enforcement investigatory records collected, maintained, and shared by ICE.

The purpose of this system of records is to collect and maintain records related to external investigations and support conducted by ICE offices, primarily HSI. ICE/HSI is the largest investigative branch of the DHS. The agency was created to more effectively

enforce immigration and customs laws and to protect the United States against terrorist attacks. ICE does this by targeting the people, money, and materials that support terrorism and other criminal activities. ICE investigates on its own and in conjunction with other agencies a broad range of illegal activities, such as terrorism, organized crime, gangs, child exploitation, and intellectual property violations.

This system of records covers information related to external audits, inquiries, and investigations pertaining to suspected violations of laws regulating the movement of people and goods into and out of the United States. For example, this system of records will include investigatory records that are generated prior to the creation of an official case file, and records pertaining to immigration status inquiries that do not constitute an official criminal investigation.

This system of records was also used to support information requests from the U.S. Congress relating to potential recipients of private immigration relief. That purpose has since been transferred to the DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER) System of Records (*see* 81 FR 72080 (October 19, 2016)). This update modifies the system of records notice to excise the stated purpose, category of individuals, and routine use that related to supplying information to assist with private immigration relief.

The following list includes the full explanation of changes to this system of records notice:

(1) The category of individuals in this system of records has been modified to include family members and known associates of a subject of investigation, as well as individuals and third-party record holders who are served administrative subpoenas and summonses for the production of records and testimony.

(2) The category of records has been modified to include criminal history, immigration status and history, biometrics (e.g., facial images, iris images, and

fingerprints), record holder information (e.g., biographical, contact), information derived from location tracking tools, License Plate Reader (LPR) information, social media information, suspicious financial activity, currency transaction reports, currency or monetary instrument reports, email addresses and the contents of email records, unique numerical identifiers assigned to biometrics, telecommunication device identifiers, telecommunications usage data, call and subscriber records, banking records, travel history records, and the statements of targets and witnesses. The categories of records will also include information pertaining to DNA tests conducted by ICE to verify a familial relationship.

(3) DHS is modifying Routine Use E and adding Routine Use F to conform to the Office of Management and Budget (OMB) Memorandum M-17-12 “Preparing for and Responding to a Breach of Personally Identifiable Information,” (Jan. 3, 2017).

(4) ICE is also adding Routine Uses I, T, and U. Routine uses following Routine Use E are being renumbered to account for these additional routine uses. The following routine uses were added to:

- (I) Allow data sharing between ICE and other federal agencies for a statistical or research purpose, including the development of methods or resources to support statistical or research activities.
- (T) Allow sharing between ICE and the Department of State (DOS) in order to support DOS in making accurate passport and visa issuance, reissuance or revocation determinations;
- (U) Allow data sharing between ICE and federal, state, local, tribal, territorial, international, or foreign government agencies or multinational governmental organizations when DHS desires to exchange relevant data for the purpose of developing, testing, or implementing new software or

technology whose purpose is related to the purpose of this system of records.

(5) ICE is removing a routine use listed in the previous SORN as Routine Use N, which permitted sharing to any person or entity to the extent necessary to prevent immediate loss of life or serious bodily injury, such as disclosure of custodial release information to witnesses who have received threats from individuals in custody. This routine use was found to be duplicative of other routine uses, and has been removed.

(6) Additionally, DHS/ICE is making non-substantive edits to the routine uses to align with previously published Department of Records Notices and in accordance with Appendix I to OMB Circular A-130, Federal Agency Responsibilities for Maintaining Records About Individuals.

(7) DHS/ICE is also correcting the records retention schedule for the system of records from 75 years, as stated in the previous publication of this SORN, to 20 years. The former retention schedule was approved by the National Archives and Records Administration (NARA) for U.S. Customs, before ICE was created. The corrected schedule currently controls ICE records management, but ICE is in the process of creating a new schedule for approval by NARA.

Lastly, this notice includes non-substantive changes to simplify formatting and text of the previously published notice.

II. Privacy Act

The Privacy Act embodies fair information principles in a statutory framework governing the means by which Federal Government agencies collect, maintain, use, and disseminate individuals' records. The Privacy Act applies to information that is maintained in a "system of records." A "system of records" is a group of any records under the control of an agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular

assigned to the individual. In the Privacy Act, an individual is defined to encompass United States citizens and lawful permanent residents. Additionally, the Judicial Redress Act (JRA) provides covered persons with a statutory right to make requests for access and amendment to covered records, as defined by the JRA, along with judicial review for denials of such requests. In addition, the JRA prohibits disclosures of covered records, except as otherwise permitted by the Privacy Act. Individuals may request access to their own records that are maintained in a system of records in the possession or under the control of DHS by complying with DHS Privacy Act regulations, 6 CFR Part 5.

The Privacy Act requires each agency to publish in the Federal Register a description denoting the type and character of each system of records that the agency maintains, and the routine uses that are contained in each system in order to make agency record keeping practices transparent, to notify individuals regarding the uses to which personally identifiable information is put, and to assist individuals to more easily find such files within the agency. Below is the description of the DHS/ICE-009 External Investigations System of Records.

In accordance with 5 U.S.C. sec. 552a(r), DHS has provided a report of this system of records to the Office of Management and Budget (OMB) and to Congress.

SYSTEM NAME AND NUMBER: U.S. Department of Homeland Security (DHS)/Immigration and Customs Enforcement (ICE)-009 External Investigations.

SECURITY CLASSIFICATION: Unclassified and Law Enforcement Sensitive (LES).

SYSTEM LOCATION: Records are maintained at U.S. Immigration and Customs Enforcement Headquarters in Washington, D.C. and in field offices.

SYSTEM MANAGER(S): Immigration and Customs Enforcement, Mission Support Division, Unit Chief, Executive Information Unit/Program Management Oversight (EIU/PMO), Potomac Center North, 500 12th Street, SW, Washington, D.C. 20536.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 5 U.S.C. 301; 6 U.S.C.

201-203; 8 U.S.C. 1357; 18 U.S.C. 116; 18 U.S.C. 554; 18 U.S.C. 1091; 18 U.S.C. 2340A; 18 U.S.C. 2441; 18 U.S.C. 2442; 18 U.S.C. 2518; 19 U.S.C. 66; 19 U.S.C. 1431; 19 U.S.C.1509; 19 U.S.C. 1603; 19 U.S.C. 2072; 21 U.S.C. 967; 22 U.S.C. 2778; 40 U.S.C. 1315; 50 U.S.C. 1701; 50 U.S.C. 2410; 50 U.S.C. 2411; other applicable authorities from Title 18, United States Code; and Title 19, United States Code as delegated by the Secretary of Homeland Security under his or her authority granted by the Homeland Security Act of 2002 (Pub. Law 107-296); 31 CFR part 103; Title 40 United States Code; INA 235(d)(4)(A); and INA 274A(e)(2)(C).

PURPOSE OF THE SYSTEM: (1) To document external audits, inquiries, and investigations performed by ICE pertaining to suspected violations of laws regulating the movement of people and goods into and out of the United States in addition to other violations of other laws within ICE's jurisdiction; (2) To facilitate communication between ICE and foreign and domestic law enforcement agencies for the purpose of enforcement and administration of laws, including immigration and customs laws; (3) To provide appropriate notification to victims in accordance with federal victim protection laws; (4) To support inquiries and investigations performed to enforce the administrative provisions of the INA; and (5) To identify potential criminal activity, immigration violations, and threats to homeland security; to uphold and enforce the law; and to ensure public safety.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Categories of individuals covered by this system include: (1) Individuals who are the subjects of current or previous law enforcement investigations into violations of U.S. customs and immigration laws, as well as other laws and regulations within ICE's jurisdiction, including investigations led by other domestic or foreign agencies in which ICE is providing support and assistance; (2) Individuals who are the subjects of investigatory referrals from other agencies, tips, and other leads acted on by ICE pertaining to potential

violations of U.S. customs and immigration law, as well as other laws and regulations within ICE's jurisdiction; (3) Individuals who are or have been the subject of inquiries or investigations conducted by ICE related to the enforcement of the employment control provisions of the Immigration and Nationality Act (INA) and related criminal statutes including individuals who are being investigated or have been investigated to determine whether their employment-related activities are in violation of the employment control provisions of the INA and/or related criminal statutes; individuals who employ others in their individual capacity whether related to a business activity or not; and individuals who have submitted completed Form I-9 (Employment Eligibility Verification Form) and other documentation to establish identity and work eligibility/authorization under the employment control provisions of the INA; (4) Family and known associates of subjects of investigation; (5) Victims and witnesses in ICE law enforcement investigations described above; (6) Individuals and third-party record holders who are served administrative subpoenas and summonses for the production of records or testimony; (7) Fugitives with outstanding federal or state warrants; (8) Operators of vehicles crossing U.S. borders who are the subject of an ICE investigation, including drivers of automobiles, private yacht masters, private pilots arriving in or leaving the United States; and (9) Regulatory and licensing agency personnel and other individuals who are involved with or supporting law enforcement investigations pertaining to U.S. export control matters conducted by ICE.

CATEGORIES OF RECORDS IN THE SYSTEM: Categories of records in this system may include:

Subject Records:

- Name and Aliases;
- Addresses;
- Social Security number;

- Armed Forces Number;
- Alien Registration number;
- Date and place of birth;
- Citizenship;
- Passport and visa information;
- License information for owners and operators of vehicles, aircraft, and vessels;
- Criminal history;
- Immigration status and history;
- Employment history or business information;
- Information related to the subject's entry and exit of the United States;
- Other biographical information;
- IP address;
- Social media account information and publicly available social media posts;
- Biometric information, including facial images, iris images, fingerprints, and voice audio;
- Suspicious financial activity, currency transaction reports, and currency or monetary instrument reports; and
- Information related to whether individuals have a verified familial relationship based on DNA test results.

Associate, Victim, and Witness Records:

- Name;
- Contact information, including address and telephone numbers;
- Alien Registration number;
- Date and place of birth;

- Citizenship;
- Passport and visa information;
- Biometric information, including facial images, iris images, fingerprints, and voice audio;
- Sworn statements, reports of interview, and testimony;
- Relationship to subject of the investigation;
- Social media handles or account names and publicly available social media posts;
- Victim services needed; and
- Other relevant biographical and background information, such as employment and education.

Location-Related Records:

- Location tracking tools that maintain a list of tracking devices by serial number/Mobile Directory Number (MDN)/International Mobile Equipment Identity (IMEI)/Mobile Equipment ID (MEID), and their current locations using Global Positioning System (GPS) and/or assisted Cellular Tower coordinates. These location tracking tools are deployed on targets of investigations, vehicles of interest in investigations, contraband, but also on the official vehicles owned by ICE and used by agents and officers in the field;
- License Plate Reader (LPR) information, including images of vehicles license plates associated with a target of investigation (a person or vehicle), date and time of image capture, and GPS coordinates for the location where the license plate was photographed;

Third-Party Records Holders:

- Name;

- Date of birth;
- Contact information, including address and telephone numbers;
- Social Security number, Alien Number, tax information number, or other personal identification numbers;
- Importer and exporter numbers;
- Internet protocol (IP) addresses and uniform resource locators (URLs);
- Bank account numbers;
- Device identifiers and serial numbers.

Investigatory and Evidentiary Records:

- ICE case number;
- Unique numerical identifiers assigned to biometrics for administrative purposes;
- Identifying information of assigned ICE personnel, including name, badge number, and contact information;
- Incident reports;
- Complaint forms and other records pertaining to potential or actual intellectual property crimes;
- I-9 Forms and other records pertaining to employment control audits, inquiries, and investigations;
- Emails;
- Telecommunication device identifiers;
- Telecommunications usage data;
- Call and subscriber records;
- Banking records;
- Travel history records;

- Reports and memoranda prepared by investigators during the course of the investigation or received from other agencies participating in or having information relevant to the investigation;
- Statements of targets and witnesses;
- Law enforcement intelligence reports;
- Electronic surveillance reports;
- Asset ownership information such as registration data and license data, for vehicles, vessels, merchandise, goods, and other assets;
- Information about duties and penalties owed, assessed, and paid;
- Information about goods and merchandise, such as import and export forms and declarations filed, lab or analytical reports, valuation and classification of goods, and other relevant data;
- Correspondence and court filings;
- Information received from other governmental agencies, confidential sources, and other sources pertaining to an investigation, as well as investigatory referrals from other agencies, tips, and other leads pertaining to potential violations of U.S. customs and immigration law, as well as other laws and regulations within ICE's jurisdiction; and
- Any other evidence in any form, including papers, photographs, video, electronic recordings, electronic data, or video records that was obtained, seized, or otherwise lawfully acquired from any source during the course of the investigation, to the extent relevant and necessary for the performance of ICE's statutory enforcement authorities.

RECORD SOURCE CATEGORIES: ICE may receive information in the course of its law enforcement investigations from nearly any source. Sources of information include: domestic and foreign governmental and quasi-governmental agencies and data systems,

public records, publicly available social media, commercial data aggregators, import and export records systems, immigration and alien admission records systems, members of the public, subjects of investigation, victims, witnesses, confidential sources, and those with knowledge of the alleged activity.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING

CATEGORIES OF USES AND PURPOSES OF SUCH USES: In addition to those disclosures generally permitted under 5 U.S.C. sec. 552a(b) of the Privacy Act, all or a portion of the records of information contained in this system may be disclosed outside DHS as a routine use pursuant to 5 U.S.C. sec. 552a(b)(3) as follows:

A. To the Department of Justice, Offices of the U.S. Attorney, or other federal agencies conducting litigation or in proceedings before any court, adjudicative, or administrative body, when it is relevant or necessary to the litigation and one of the following is a party to the litigation or has an interest in such litigation:

1. DHS or any component thereof;
2. Any employee or former employee of DHS in his/her official capacity;
3. Any employee or former employee of DHS in his/her individual capacity, only when DOJ or DHS has agreed to represent the employee; or
4. The United States or any agency thereof.

B. To a congressional office from the record of an individual in response to an inquiry from that congressional office made at the request of the individual to whom the record pertains.

C. To the National Archives and Records Administration (NARA) or the General Services Administration pursuant to records management inspections being conducted under the authority of 44 U.S.C. secs. 2904 and 2906.

D. To an agency or organization for the purpose of performing audit or oversight operations as authorized by law, but only such information as is necessary and relevant to

such audit or oversight function.

E. To appropriate agencies, entities, and persons when (1) DHS suspects or has confirmed that there has been a breach of the system of records; (2) DHS has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, DHS (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with DHS's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

F. To another Federal agency or Federal entity, when DHS determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

G. To an appropriate federal, State, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, where a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations and such disclosure is proper and consistent with the official duties of the person making the disclosure.

H. To contractors and their agents, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for DHS, when necessary to accomplish an agency function related to this system of records. Individuals provided information under this routine use are subject to

the same Privacy Act requirements and limitations on disclosure as are applicable to DHS officers and employees.

I. To a federal agency for a statistical or research purpose, including the development of methods or resources to support statistical or research activities, provided that the records support DHS programs and activities that relate to the purpose(s) stated in this SORN, and will not be used in whole or in part in making any determination regarding an individual's rights, benefits, or privileges under federal programs, or published in any manner that identifies an individual.

J. To third parties during the course of a law enforcement investigation to the extent necessary to obtain information pertinent to the investigation, provided disclosure is appropriate to the proper performance of the official duties of the officer making the disclosure.

K. To federal law enforcement and/or regulatory agencies, technical, or subject matter expert, or any other entity involved in or assisting with law enforcement efforts pertaining to suspected or confirmed export violations in accordance with Federal export laws, including the Arms Export Control Act, 22 U.S.C. sec. 2778 and the Export Administration Act, 50 U.S.C. sec. 2410.

L. To federal and foreign government intelligence or counterterrorism agencies or components when DHS becomes aware of an indication of a threat or potential threat to national or international security, or when such disclosure is to support the conduct of national intelligence and security investigations or to assist in anti-terrorism efforts.

M. To victims regarding custodial information, such as release on bond, order of supervision, removal from the United States, or death in custody, about an individual who is the subject of a criminal or immigration investigation, proceeding, or prosecution.

N. To international, foreign, intergovernmental, and multinational government agencies, authorities, and organizations in accordance with law and formal or informal international arrangements.

O. To a public or professional licensing organization when such information indicates, either by itself or in combination with other information, a violation or potential violation of professional standards, or reflects on the moral, educational, or professional qualifications of an individual who is licensed or who is seeking to become licensed.

P. To federal, state, local, tribal, territorial, or foreign government agencies or organizations, or international organizations, lawfully engaged in collecting law enforcement intelligence, whether civil or criminal, to enable these entities to carry out their law enforcement responsibilities, including the collection of law enforcement intelligence.

Q. To the Department of State when it requires information to consider and/or provide an informed response to a request for information from a foreign, international, or intergovernmental agency, authority, or organization about an alien or an enforcement operation with transnational implications.

R. To federal, state, local, territorial, tribal, international, or foreign criminal, civil, or regulatory law enforcement authorities when the information is necessary for collaboration, coordination, and de-confliction of investigative matters, prosecutions, and/or other law enforcement actions to avoid duplicative or disruptive efforts and to ensure the safety of law enforcement officers who may be working on related law enforcement matters.

S. To the Department of Justice to facilitate the missions of the Organized Crime Drug Enforcement Task Force (OCDETF) Program and the International Organized Crime Intelligence and Operations Center (IOC-2).

T. To the Department of State for use in passport and visa revocation, issuance, or reissuance determinations.

U. To appropriate federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations, with the approval of the Chief Privacy Officer, when DHS is aware of a need to use relevant data for purposes of testing new technology to be used by or on behalf of DHS.

V. To the news media and the public, with the approval of the Chief Privacy Officer in consultation with counsel, when there exists a legitimate public interest in the disclosure of the information, when disclosure is necessary to preserve confidence in the integrity of DHS, or when disclosure is necessary to demonstrate the accountability of DHS's officers, employees, or individuals covered by the system, except to the extent the Chief Privacy Officer determines that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: Records in this system are stored electronically or on paper in secure facilities in a locked drawer behind a locked door. The records are stored on magnetic disc, tape, digital media, and CD-ROM.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Records are retrieved by individual's name, date of birth, ICE investigative file number, Social Security number, numerical identifiers assigned to biometrics collected (e.g., fingerprint ID number); driver's license number, pilot's license number, vehicle license plate number, address, home telephone number, passport number, citizenship, country of birth, armed forces number, and date of entry into the United States.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: Investigative files concerning munitions control cases are permanent records that are transferred to the Federal Records Center after one year, and then

transferred to NARA fifteen years after case closure, in accordance with legacy Customs schedule N1-36-86-1/162.38. Records for all other closed investigative cases are retained for 20 years in accordance with legacy customs schedule N1-36-86-1-161.3 (inv 7B). Destruction is by burning or shredding. An updated schedule for investigative records will be developed and submitted to NARA for approval.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: DHS/ICE safeguards records in this system according to applicable rules and policies, including all applicable DHS automated system security and access policies. DHS/ICE has imposed strict controls to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions. The system maintains a real-time auditing function of individuals who access the system. Additional safeguards may vary by component and program.

RECORD ACCESS PROCEDURES: The Secretary of Homeland Security has exempted this system from the notification, access, and amendment procedures of the Privacy Act because it is a law enforcement system. However, ICE will consider requests to determine whether or not information may be released. Thus, individuals seeking notification of and access to any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the U.S. Immigration and Customs Enforcement Freedom of Information Act (FOIA) Officer, whose contact information can be found at <http://www.dhs.gov/foia> under "Contact Information." If an individual believes more than one component maintains Privacy Act records concerning him or her, the individual may submit the request to the Chief Privacy Officer and Chief Freedom of Information Act Officer, U.S. Department of Homeland Security, 245 Murray Drive SW, Building 410, STOP-0550, Washington, D.C. 20528. Even if neither the Privacy Act nor

the Judicial Redress Act provides a right of access, certain records about you may be available under the Freedom of Information Act.

When an individual is seeking records about himself or herself from this system of records or any other Departmental system of records, the individual's request must conform with the Privacy Act regulations set forth in 6 CFR Part 5. The individual must first verify his/her identity, meaning that the individual must provide his/her full name, current address, and date and place of birth. The individual must sign the request, and the individual's signature must either be notarized or submitted under 28 U.S.C. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, you may obtain forms for this purpose from the Chief Privacy Officer and Chief Freedom of Information Act Officer, <http://www.dhs.gov/foia> or 1-866-431-0486. In addition, the individual should:

- Explain why he or she believes the Department would have information being requested;
- Identify which component(s) of the Department he or she believes may have the information;
- Specify when the individual believes the records would have been created; and
- Provide any other information that will help the FOIA staff determine which DHS component agency may have responsive records.

If the request is seeking records pertaining to another living individual, the request must include an authorization from the individual whose record is being requested, authorizing the release to the requester.

Without the above information, the component(s) may not be able to conduct an effective search, and the individual's request may be denied due to lack of specificity or lack of compliance with applicable regulations.

CONTESTING RECORD PROCEDURES: For records covered by the Privacy Act or

covered JRA records, individuals may make a request for amendment or correction of a record of the Department about the individual by writing directly to the Department component that maintains the record, unless the record is not subject to amendment or correction. The request should identify each particular record in question, state the amendment or correction desired, and state why the individual believes that the record is not accurate, relevant, timely, or complete. The individual may submit any documentation that would be helpful. If the individual believes that the same record is in more than one system of records, the request should state that and be addressed to each component that maintains a system of records containing the record.

Individuals who wish to contest the accuracy of records in this system of records should submit these requests to the Privacy Division of the ICE Information Governance & Privacy Office. Requests must comply with verification of identity requirements set forth in Department of Homeland Security Privacy Act regulations at 6 CFR 5.21(d). Please specify the nature of the complaint and provide any supporting documentation. By mail (please note substantial delivery delays exist): ICE Information Governance & Privacy Office, ATTN: Privacy Division, 500 12th Street SW, Mail Stop 5004, Washington, D.C. 20536. By email: ICEPrivacy@ice.dhs.gov.

Please contact the Privacy Division with any questions about submitting a request at (202) 732-3300 or ICEPrivacy@ice.dhs.gov.

NOTIFICATION PROCEDURES: See “Record Access Procedures” above.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: The Secretary of Homeland Security, pursuant to 5 U.S.C. sec. 552a(j)(2), has exempted this system from the following provisions of the Privacy Act: 5 U.S.C. sec. 552a(c)(3), (c)(4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(5), and (e)(8); (f); and (g). Additionally, the Secretary of Homeland Security, pursuant to 5 U.S.C. sec. 552a(k)(2), has exempted this system from the following provisions of the Privacy Act: 5 U.S.C. sec. 552a(c)(3); (d);

(e)(1), (e)(4)(G), and (e)(4)(H); and (f). To the extent a record contains information from other exempt systems of records, ICE will rely on the exemptions claimed for those systems.

HISTORY: DHS/ICE-009 External Investigations, 75 FR 404 (January 5, 2010).

Constantina Kozanas,
Chief Privacy Officer,

U.S. Department of Homeland Security.

[FR Doc. 2020-25619 Filed: 11/19/2020 8:45 am; Publication Date: 11/20/2020]